Software-Defined Reconfigurability, White Boxes, and Abstraction

Nicola Sambo[✉], Alessio Giorgetti, Andrea Sgambelluri, Piero Castoldi, and Luca Valcarenghi

Scuola Superiore Sant'Anna, Pisa, Italy
nicola.sambo@santannapisa.it

Abstract. Next generation networks – spanning from wide area networks to intra-datacenters – are expected to encompass devices and sub-devices from different vendors. Inter operability and vendor neutrality are now key topics for researchers and companies as a way to reduce costs avoiding to be tied to a single vendor. Also the management system is expected to be disaggregated from the hardware and possibly developed by a different company. An example is the *white box*, which disaggregates the software from the hardware and can be composed of modules from different vendors. Currently, NETCONF – based on YANG – is the protocol considered for the (re)configuration of white boxes. Discussions are being carried on to identify commonly agreed information models to guarantee vendor-neutral configuration and management of next generation networks.

In addition, emerging services (e.g., 5G) will impose the involvement of a variety of technologies (e.g., networks, datacenters) and resources (e.g., compute, storage, radio). Such heterogeneity will imply the cooperation of several business actors to bring services to the users. In such a scenario, the management of resources will require their abstraction in order to satisfy confidentiality as well as to increase scalability and, again, to provide information that is neutral with respect to the related vendor and technology.

In this paper, we propose to use NETCONF also for the exchange of resource information among different business actors considering the several network segments (wide area network, data centers, radio segment) involved in a 5G vertical. To this purpose, resource abstraction is proposed based on a YANG data model. An experiment will involve the (re)configuration of a wide area network composed of white boxes. Moreover, resource information (virtual links) will be exchanged through NETCONF with the objective of orchestrating resources.

Keywords: 5G · White box · Disaggregated networks · YANG · NETCONF

1   Introduction

In the last years, a lot of interest within research and market has been directed to vendor-neutrality, inter-operability, and disaggregation of software from the hardware [1]. This movement started from network operators and service providers with the objective of removing the traditional vendor-lock-in of their networks. Indeed, up to now, multi-vendor-interoperability is not guaranteed, thus network upgrades must be performed by the same vendor. Similarly, the management system is tied to the network and typically proprietary of the vendor. These limitations impede the market. Inter-operability and vendor-neutral control and management permit operators and service providers to lower the costs avoiding to be tied to a single vendor and adopting the best of breed technologies. An example is the *white box* [2,3], a node disaggregating the hardware from the software (e.g., management systems) that can also be assembled by modules from different vendors. The control of white box is performed via the NETCONF protocol [4] supporting vendor-neutral YANG data models [5–8].

In addition, emerging services such as automotive, e-health, video streaming, documentation of mega events will be supported through the coordination of several heterogeneous technologies in different network segments. Datacenters, radio, and network technologies will be involved in the service delivery to the user requiring the cooperation of different business actors, each one administrating a network segment [9]. Such business actors will have to exchange their domain information (e.g., latency) so that services can be orchestrated. In such a scenario, the management of resources in play will require their abstraction (i.e., a simplification exchanging a reduced set of information) [10] in order to satisfy confidentiality as well as to increase scalability and provide information that is neutral with respect to the related vendor and technology. In particular, regarding resources, 5G services will exploit *network slice*: i.e., a set of virtualized functions, connectivity, compute, and storage resources [11]. The European Telecommunications Standards Institute (ETSI) is defining standard interfaces to enable domain managers (each belonging to the related company) in the exchange of their resource information (e.g., abstracted connectivity and compute resources) [12].

In this paper, we will first describe the NETCONF protocol (which operates in a client/server way) and its use for the (re)configuration of a white box acted by a Software Defined Networking (SDN) controller. Then, we will propose to exploit NETCONF also to manage abstracted domain information in a 5G scenario, leveraging the native characteristics of NETCONF in handling servers. An experiment will be presented showing the configurability of a wide area network (WAN) based on white boxes. The information exchanged between the different business actors will permit to set up resources satisfying the proper level of quality of service (in terms of latency). To this purpose, reconfiguration will be acted without exchanging information about the technology or detailed information of the network.
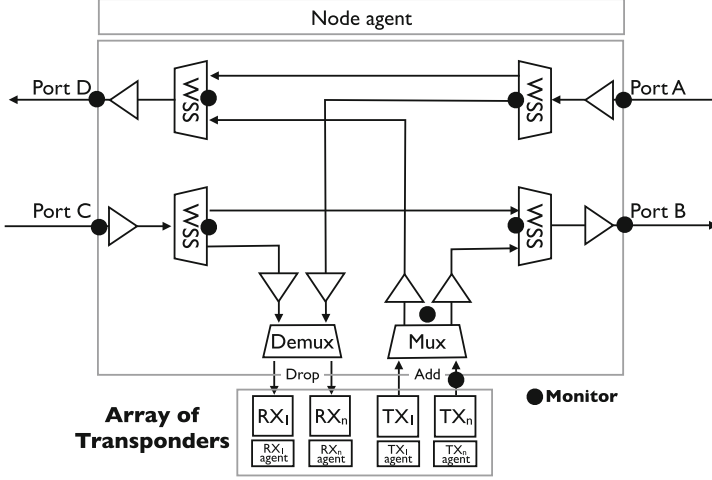
Fig. 1. White box

Table 1. Server describing configuration parameters of a cross connection

Parameter	Value
Input port	C
Output port	B
Central frequency	193.1
Width	37.5

2   NETCONF for White Box Configuration

A wide area network (WAN) based on flexible grid optical technology is assumed. In such a network scenario, white boxes (as the one shown in Fig. 1) assembled with several transponders, monitors, and filters (wavelength selective switches—WSSs) for switching and add/drop is considered as in [2]. The agent is the interface with the SDN controller. Regarding monitors, WSSs support the power monitor per channel, then other power monitors can be placed in the incoming and outgoing ports to measure the total channel power of the lines, as well as at the input and output of transponders. More advanced monitors (e.g., for filtering effects [2]) can be also assumed.

NETCONF, operating in a client server way, is responsible for the (re)-configuration of the white box. More specifically, NETCONF messages write or reports parameters' values stored into a server describing the configuration and the state of the white box. Such server reflects the information model describing the white box through a set of parameters. NETCONF messages contain fields associated to these parameters. In particular, *configuration* parameters are written to the proper configuration values via the NETCONF <edit-config> message. Table 1 shows an entry of the server related to a node cross-connection.

**Table 2.** Server describing configuration parameters of a transponder

Parameter	Value
net bit rate	100
baudrate	28
modulation format	pm-qpsk
FEC	7
launch power	0
central frequency	193.1

Table 3. State parameters of a transponder

Parameter	Value
pre-FEC BER	0.00213
osnr	16.4
cd	5133
pmd	5.19
B	33.2

In particular, the NETCONF <edit-config> message, sent from the SDN controller to the agent, writes the values of the proper parameters: input and output ports, and the frequency slot characterized by a central frequency (in THz) and a width (in GHz). Then, the agent is responsible to locally act, according to these entries, the cross connection configuration by properly configuring the WSSs. In the case of transponders, the <edit-config> message writes into the server the configuration parameters of a specific transponder (identified with an id). An example of configured values is reported in Table 2: net bit rate to 100 Gb/s achieved with polarization multiplexing quadrature phase shift keying (PM-QPSK) modulation format, 7% of forward error correction (FEC), and 28 Gbaud of symbol rate, at a central frequency of 193.1 THz with a launch power of 0 dBm.

Then, besides configuration parameters, even *state* parameters are included. They can only be read and are typically used to describe monitoring information. There are two ways to report monitoring information to an SDN controller. The SDN controller can send a <get> message to the agent requesting for the value of a specific parameter. The second way is asynchronous and based on a subscription and notification mechanism. The SDN controller, through the <create-subscription> message, asks to be notified when a state parameter exceeds a given value decided by the SDN controller. Table 3 shows parameters monitored by a transponder through the coherent receiver: pre-FEC bit error rate (pre-FEC BER), optical signal to noise ratio (OSNR), chromatic dispersion (CD), polarization mode dispersion (PMD), and signal bandwidth B. Then, other servers will be present for power monitors.
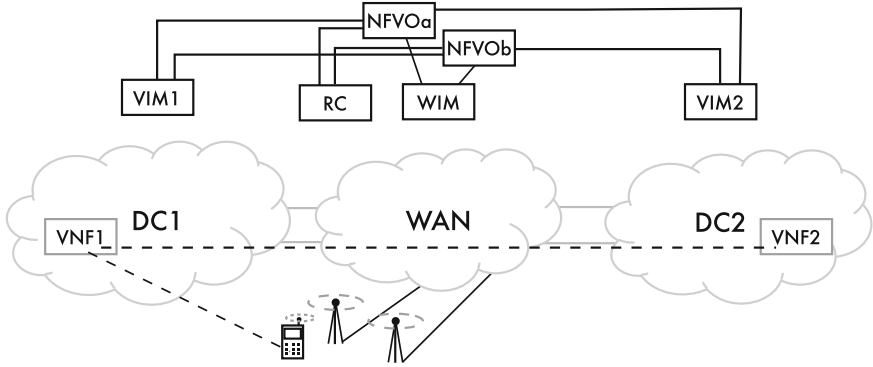
Fig. 2. Scenario involving multiple network technologies and domains

The next section describes how NETCONF messages can be used also for exchanging information about different network segments hiding the technology.
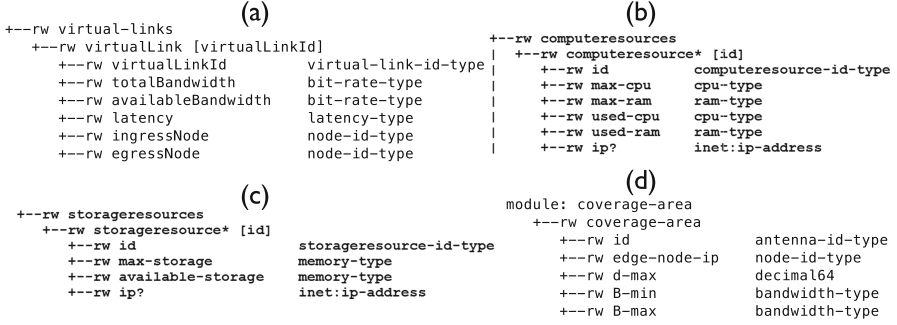
3   NETCONF for Slice Management

3.1   Scenario Description

The considered scenario is shown in Fig. 2. A user identified with a mobile phone exploits a service delivered by connecting the user to two virtual network functions (VNFs). This connection is enabled by virtual links involving the radio segment, the WAN, and data centers. VNFs are created using virtual storage and compute resources of datacenters. A Network Function Virtualization Orchestrator (NFVO), associated with a service provider, is responsible to orchestrate all the network, storage, and compute resources of each domain with the objective of satisfying quality of service (QoS). Several service providers exploits a network and each provider holds an NFVO (NFVO$_a$ and NFVO$_b$ in Fig. 2). Each domain can belong to a different business actor and is coordinated by a manager with the view of all the resources. In particular, the WAN Infrastructure Manager (WIM) [12] is responsible for the WAN, a Virtual Infrastructure Manager (VIM) [12] for a datacenter, and a Radio Controller (RC) for the radio. Each WIM, VIM, RC have the detailed view of their domain and can rely on an SDN controller for (re)configuring the domain.

3.2   Slice Management Through NETCONF

According to the slice definition, slice management implies the management of network, storage, compute, and radio resources. ETSI defined a set of interfaces to enable a consumer block (the NFVO) to *query* information about virtual network, storage, and compute resources to the VIM [12] to *reserve*, *allocate*, and *terminate* such resources. Moreover, an NFVO can also *subscribe* to *notifications*

```
                         (a)                                        (b)
  +--rw virtual-links                           +--rw computeresources
    +--rw virtualLink [virtualLinkId]           |  +--rw computeresource* [id]
       +--rw virtualLinkId       virtual-link-id-type |     +--rw id          computeresource-id-type
       +--rw totalBandwidth      bit-rate-type   |     +--rw max-cpu      cpu-type
       +--rw availableBandwidth  bit-rate-type   |     +--rw max-ram      ram-type
       +--rw latency             latency-type    |     +--rw used-cpu     cpu-type
       +--rw ingressNode         node-id-type    |     +--rw used-ram     ram-type
       +--rw egressNode          node-id-type    |     +--rw ip?          inet:ip-address

                         (c)                                        (d)
                                                     module: coverage-area
  +--rw storageresources                               +--rw coverage-area
    +--rw storageresource* [id]                            +--rw id          antenna-id-type
       +--rw id               storageresource-id-type      +--rw edge-node-ip  node-id-type
       +--rw max-storage      memory-type                  +--rw d-max       decimal64
       +--rw available-storage  memory-type                +--rw B-min       bandwidth-type
       +--rw ip?              inet:ip-address              +--rw B-max       bandwidth-type
```

Fig. 3. YANG data models for abstracted (a) virtual link, (b) compute, (c) storage resources, and (d) coverage area.

if the state of some resource changes and also if some performance parameter falls in a critical range. Network interfaces defined for the VIM are also considered between NFVO and WIM [13]. Based on the ETSI interfaces and operations, in this paper, we propose to use NETCONF to manage resource information about each domain, given the nature of this protocol in manipulating information stored into a server.

– <get> message: it can be used by the NFVO to query information about abstracted resources: virtual network topology (in the form of a list of virtual links), virtual compute and storage resources, radio coverage area
– <rpc-reply> message: upon query, this message can be used by a manager (e.g., WIM) to inform about abstracted resources. Figure 3 shows our own-developed YANG models describing the abstracted virtual link, compute, and storage resources and the radio coverage area. The virtual link is described with an identifier, with the IP addresses of ingress and egress nodes, an overall cumulated latency, and the total and available bandwidth. The whole path connecting the ingress and egress nodes, as well as the used technology, is hidden to NFVO (for scalability or confidentiality reasons), while WIM maintains the complete view of its WAN. Storage resources are mainly described by storage values (maximum and available), while compute resources by CPU and RAM. The radio coverage area is described by a maximum distance (d-max) covered by the antenna and by a maximum and minimum bandwidth that can be used for a service in this coverage area. The maximum bandwidth is computed in proximity of the antenna, while the minimum one is at d-max. These values depend on propagation models, in particular on the signal-to-interference-noise-ratio, sometimes translated into a parameter named Channel Quality Indicator (CQI) [14]
– <rpc> custom message: once the NFVO has decided for a specific resource (e.g., a virtual link characterized by the proper latency), this message is used to request a manager for the allocation of a specific resource. Then, the manager, as an example the WIM, handles the allocation by relying on an SDN

controller setting up (thus configuring white box in our case) a new lightpath
between the ingress and egress pairs

– <create-subscription> message: an NFVO (e.g., $NFVO_a$ of Fig. 2) can request
to a manger to be notified if a virtual resource changes (e.g., due to a service
associated to $NFVO_b$ of Fig. 2) or if a monitored parameter falls in a critical
range

– <notification> message: it is sent by the manager (e.g., a VIM) to NFVO if
the event at the previous item occurs

Such use of the NETCONF protocol embraces the new trends of describing
network elements and resources in a vendor-neutral way. Moreover, the abstrac-
tion models shown in Fig. 3 permit to describe all the resources in play also
in a technology-neutral way. Indeed, regarding virtual link resources, NFVO is
agnostic with respect to the technology that could be layer-3, optical, or any
other. Thus, confidentiality reasons, vendor-neutrality, and also scalability are
guaranteed.

4   Experimental Demonstration

The experiment is focused on the WAN and involves a WIM and a NFVO (for
more details about an implementation related to the exchange of information
from a VIM, the reader can refer to [15]). WIM relies on an ONOS SDN con-
troller [16] for WAN (re)configuration. The data plane is emulated except a node,
which is based on a Lumentum white box actually configured and reconfigured.
Emulated devices are associated to NETCONF servers based on ConfD [17] stor-
ing the YANG parameters describing each device. The WAN topology is shown
in Fig. 4. A service sensible to the latency is considered. NFVO requests an
abstracted topology to WIM between the nodes with IP addresses 10.10.255.9
(the white box) and 10.10.255.6. At this stage, we forced the network to have
just one route (shown in Fig. 4) between the two nodes. WIM replies with the
message shown in Fig. 5 reporting the available virtual link (with identifier 20)
characterized by a latency of 10.0 ms. NFVO evaluates such latency as critical
but, given the presence of just this virtual link, NFVO selects it. Then, ONOS
establishes the considered lightpath. Figure 6 shows the cross-connection infor-
mation at the agent of the white box. Note that the XML content is based on
a model proprietary of Lumentum, which describes the frequency slot with a
start-frequency and a end-frequency instead of a central frequency and a width.
Figure 6 also shows the input port 5101 and the output port 5202. Given that as
policy NFVO prefers virtual links with shorter latency, NFVO periodically inter-
rogates the WIM about the possibility to use another virtual link with shorter
latency. At this stage we freed resources along an alternative route in the WAN.
Consequently, WIM replies to NFVO with another available virtual link (with
identifier 21). The related message is shown in Fig. 7 reporting the latency value
of 8.5 ms and the same node pairs. Thus, NFVO can request to switch the ser-
vice to the other virtual link exploiting a make-before-break approach. The new
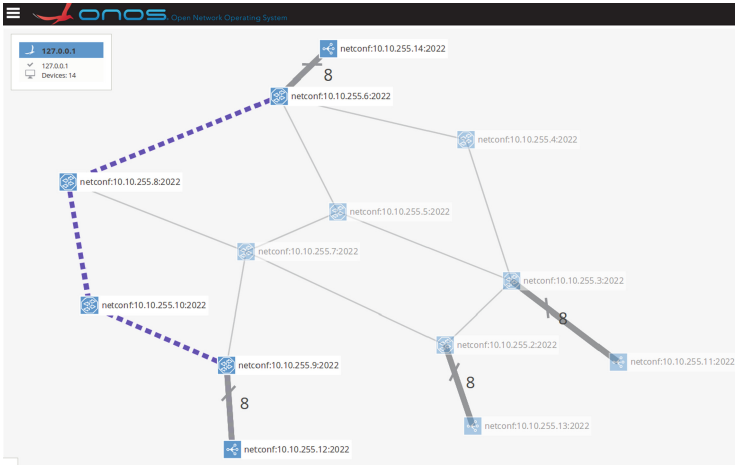
Fig. 4. WAN topology and lightpath associated to the first virtual link.

```
<virtualLink>
<virtualLinkId>20</virtualLinkId>
<totalBandwidth>100</totalBandwidth>
<availableBandwidth>100</availableBandwidth>
<latency>10.0</latency>
<ingressNode>10.10.255.9</ingressNode>
<egressNode>10.10.255.6</egressNode>
</virtualLink>
```

Fig. 5. <rpc-reply> sent by WIM to NFVO reporting the available virtual link.

route is shown in Fig. 8, while Fig. 9 shows the cross-connection information at the agent of the white box after reconfiguration. With respect to Figs. 6 and 9 shows a different output port (5201), which is the ones attached to the intermediate node 10.10.255.7. The make-before-break approach is implemented by the NFVO by requesting to WIM the allocation of a new virtual link and, once getting the acknowledgement, by terminating the old virtual link. Figure 10 shows the custom <rpc> including the identifier 21 to allocate the second virtual link, while Fig. 11 shows the custom <rpc> including the identifier 20 to terminate the second virtual link.

```
<start-freq>193675.00</start-freq>
<end-freq>193725.00</end-freq>
<attenuation>10.0</attenuation>
<blocked>false</blocked>
<power-target>0.00</power-target>
<power-target-tolerance>0.00</power-target-tolerance>
<input-port-reference>ne=1;chassis=1;card=1;port=5101
</input-port-reference>
<output-port-reference>ne=1;chassis=1;card=1;port=5202
</output-port-reference>
```
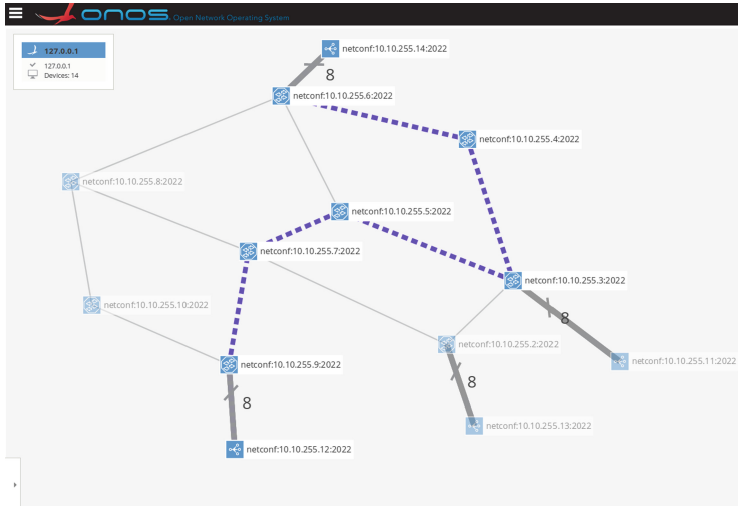
Fig. 6. Cross connection information at the agent of the destination edge associated to the first virtual link.

```
<virtualLink>
<virtualLinkId>21</virtualLinkId>
<totalBandwidth>100</totalBandwidth>
<availableBandwidth>100</availableBandwidth>
<latency>8.5</latency>
<ingressNode>10.10.255.9</ingressNode>
<egressNode>10.10.255.6</egressNode>
</virtualLink>
```

Fig. 7. <rpc-reply> sent by WIM to NFVO reporting the second virtual link.

Fig. 8. WAN topology and lightpath associated to the second virtual link.

```
<start-freq>193675.00</start-freq>
<end-freq>193725.00</end-freq>
<attenuation>10.0</attenuation>
<blocked>false</blocked>
<power-target>0.00</power-target>
<power-target-tolerance>0.00</power-target-tolerance>
<input-port-reference>ne=1;chassis=1;card=1;port=5101
</input-port-reference>
<output-port-
reference>ne=1;chassis=1;card=1;port=5201
</output-port-reference>
```

Fig. 9. Cross connection information at the agent of the destination edge associated to the second virtual link.

```
<add-connection xmlns="http://sssup.it/wim">
<virtualLinkId>21</virtualLinkId>
<ingressNode>10.10.255.9</ingressNode>
<egressNode>10.10.255.6</egressNode>
</add-connection>
```

Fig. 10. <rpc> sent by NFVO to WIM to allocate the second virtual link.

```
<terminate-connection xmlns="http://sssup.it/wim">
<virtualLinkId>20</virtualLinkId>
<ingressNode>10.10.255.9</ingressNode>
<egressNode>10.10.255.6</egressNode>
</terminate-connection>
```

Fig. 11. <rpc> sent by NFVO to WIM to terminate the first virtual link.

5   Conclusions

This paper presented the NETCONF protocol for the (re)configuration of white boxes. A different use of NETCONF was also introduced considering a 5G/inter-datacenter scenario where a service is supported by an heterogeneity of resources (e.g., network, storage) and network domains. In such a scenario service orchestration requires the knowledge of resources at each domain to properly select them. However, given the presence of different business actors involved, resources must be abstracted and some information hidden. Abstraction of networks, datacenters, and radio coverage area were here provided. Thus, we proposed to use the NETCONF protocol not only for configuration but also for the exchange of abstracted resource information (e.g., virtual link) between the several managers in play. An experiment focused on the wide area network was presented. In the experiment a service orchestrator (NFVO) interacts with the manager of the wide area network (WIM) with the objective of obtaining a virtual link guaranteeing a proper latency value, thus the QoS. Future works will be focused on the information exchange between NFVO and the radio controller. Then, the

objective is to provide an overall demo involving radio segment, wide area network, and datacenters.

References

1. Riccardi, E., Gunning, P., de Dios, O.G., Quagliotti, M., Lopez, V., Lord, A.: An operator view on the introduction of white boxes into optical networks. J. Lightwave Technol. **36**(15), 3062–3072 (2018)
2. Sambo, N., et al.: Experimental demonstration of a fully disaggregated and automated white box comprised of different types of transponders and monitors. J. Lightwave Technol. **37**(3), 824–830 (2018)
3. Velasco, L., et al.: Building autonomic optical whitebox-based networks. J. Lightwave Technol. **36**(15), 3097–3104 (2018)
4. Enns, R., Bjorklund, M., Schoenwaelder, J., Bierman, A.: IETF RFC 6241, June 2011
5. Bjorklund, M.: IETF RFC 6020
6. Dallaglio, M., Sambo, N., Cugini, F., Castoldi, P.: YANG models for vendor-neutral optical networks, reconfigurable through state machine. IEEE Commun. Mag. **55**(8), 170–178 (2017)
7. In http://www.openconfig.net
8. In http://www.openroadm.org
9. Iovanna, P., et al.: 5G mobile transport and computing platform for verticals. In: 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 266–271, April 2018
10. Fiorani, M., Rostami, A., Wosinska, L., Monti, P.: Abstraction models for optical 5G transport networks. IEEE/OSA J. Opt. Commun. Networking **8**(9), 656–665 (2016)
11. ETSI GR NFV-EVE 012 v3.1.1. ETSI standard (2017)
12. ETSI GS NFV-IFA 005 v2.1.1. ETSI standard (2016)
13. ETSI GS NFV-IFA 022 v3.1.1. ETSI standard (2018)
14. ETSI TS 136 213 V13.0.0. ETSI standard (2016)
15. Sgambelluri, A., et al.: Provisioning RAN as a service (RANaaS) connectivity in an optical metro network through NETCONF and YANG. In: 2018 European Conference on Optical Communication (ECOC), pp. 1–3, September 2018
16. In https://onosproject.org/
17. In http://www.confd.io/